Spins als Träger von Quanteninformation

Joachim Stolze
Fakultät Physik, Technische Universität Dortmund, 44221 Dortmund
joachim.stolze@tu-dortmund.de

13. Juli 2019

- Was ist Spin?
- Ist Spin anschaulich?
- Hilbertraum und Quanteninformation
- Anwendungen von Quanteninformation

Spin ???

- Topspin und Backspin in (Tisch-) Tennis und anderen Sportarten
- Rotation des Balls bewirkt Änderung der Flugbahn und des Aufpralls
  → Verwirrung des Gegners
- Physikalisches Maß für Rotation:
  Drehimpuls

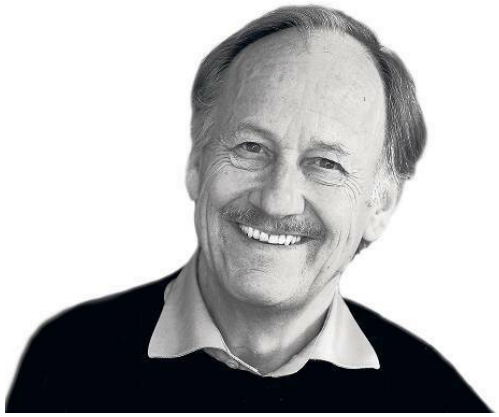
Bild:
GettyImages-182057886-56e114d65f9b5854a9f87407.jpg

(How to Execute a Volleyball Serve with Topspin)

Verwirrung durch Spin

Übungen zum integrierten Kurs *Physik IV*, Sommersemester 1979:

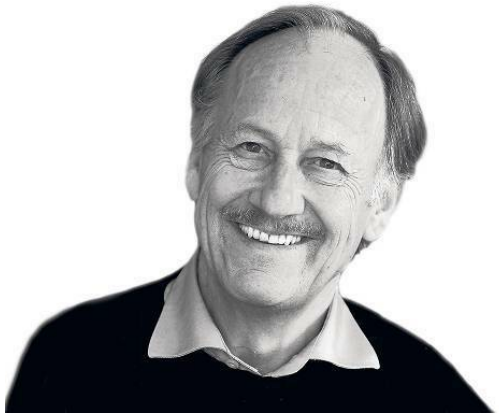
02507	Physik IV für Physiker (5 PV)		
	Mo 8.15–10.00	HG II (HBF) / HS 2	
	Mi 8.15– 9.00	HG II (HBF) / HS 1	Brandt
	Fr 11.15–13.00	HG II (HBF) / HS 2	Kleinknecht
02508	Übungen zur Physik IV für Physiker (Diplom) (4 PÜ)		
	Di 11.15–13.00	HG II (HBF) / HS 2	Brandt
		P/SR P1–01–306	Kleinknecht
	Do 14.15–16.00	CT/HS ZE 01	Stähler
		CT/HS ZE 02	Stolze



Verwirrung durch Spin

Übungen zum integrierten Kurs *Physik IV*, Sommersemester 1979:

02507	Physik IV für Physiker (5 PV)		
	Mo 8.15–10.00	HG II (HBF) / HS 2	
	Mi 8.15– 9.00	HG II (HBF) / HS 1	Brandt
	Fr 11.15–13.00	HG II (HBF) / HS 2	Kleinknecht
02508	Übungen zur Physik IV für Physiker (Diplom) (4 PÜ)		
	Di 11.15–13.00	HG II (HBF) / HS 2	Brandt
		P/SR P1–01–306	Kleinknecht
	Do 14.15–16.00	CT/HS ZE 01	Stähler
		CT/HS ZE 02	Stolze



„Herr Kleinknecht sagt, er weiß, was ein Spin ist;
Herr Brandt sagt, er weiß das nicht.
Was sollen wir denn jetzt glauben?“

Drehimpuls klassisch und quantenmechanisch

Klassisches Teilchen auf einer Kreisbahn:

$|\vec{L}| = mvr \quad \vec{L} \perp$ Bahnebene.

Bild:

Erhaltung des Drehimpulses $\Longrightarrow$ 2. Keplergesetz.
Auch zusammengesetzte Objekte können einen Drehimpuls haben,
z.B. die Erde.
Soweit alles ganz einfach.

Lernhelfer.de: Drehimpuls

Drehimpuls klassisch und quantenmechanisch

Klassisches Teilchen auf einer Kreisbahn:

$$|\vec{L}| = mvr \quad \vec{L} \perp \text{ Bahnebene.}$$

Bild:

Erhaltung des Drehimpulses $\Longrightarrow$ 2. Keplergesetz.
Auch zusammengesetzte Objekte können einen Drehimpuls haben, z.B. die Erde.
Soweit alles ganz einfach.

Lernhelfer.de: Drehimpuls

Ein quantenmechanisches Teilchens auf einer „Kreisbahn“ besitzt einen quantisierten Drehimpuls, der nur ganz bestimmte endlich viele Werte annehmen kann. Die quantenmechanische Einheit des Drehimpulses ist die durch 2π dividierte Plancksche Konstante $\hbar$:

Bild:

Illustration eines Atoms aus: Bild der Wissenschaft

$$\hbar = \frac{h}{2\pi} = 1.055 \cdot 10^{-34}\text{Js}.$$

Größenordnungen

$\hbar <<<<<$ Messgenauigkeit jedes Alltags-Geräts $\Rightarrow$ Drehimpuls-Quantisierung irrelevant im Alltag.

Die Erde: $m = 6 \cdot 10^{24}$kg, $r = 6.4 \cdot 10^{6}$m, 1 Umdrehung pro Tag:

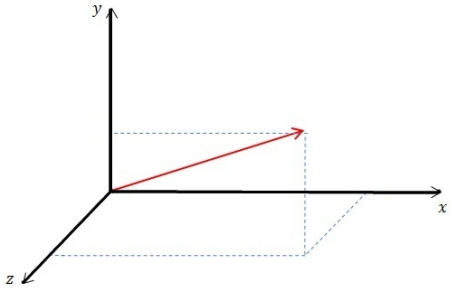
$$|\vec{L}| = 7 \cdot 10^{33}\text{Js} = 6.7 \cdot 10^{67}\hbar.$$

Etwas kleiner: $m = 1$mg, $r = 1$mm, 2 Umdrehungen pro Tag: Stundenzeiger einer sehr zarten Damen-Armbanduhr:

$$|\vec{L}| = 1.3 \cdot 10^{20}\hbar.$$

A propos Messen...

Der Drehimpuls ist ein Vektor, hat also drei Komponenten, in $x-$, $y-$ und $z-$Richtung, die man einzeln ausmessen kann, jedenfalls klassisch.



In der Quantenmechanik kann man nicht alle drei Komponenten ausmessen, da die zugrundeliegenden Größen Ort und Impuls nicht miteinander kompatibel sind, woraus auch die Heisenbergsche Unbestimmtheitsbeziehung folgt.

$$\vec{L} = \vec{r} \times \vec{p}$$

$$\vec{p} = m\vec{v}$$

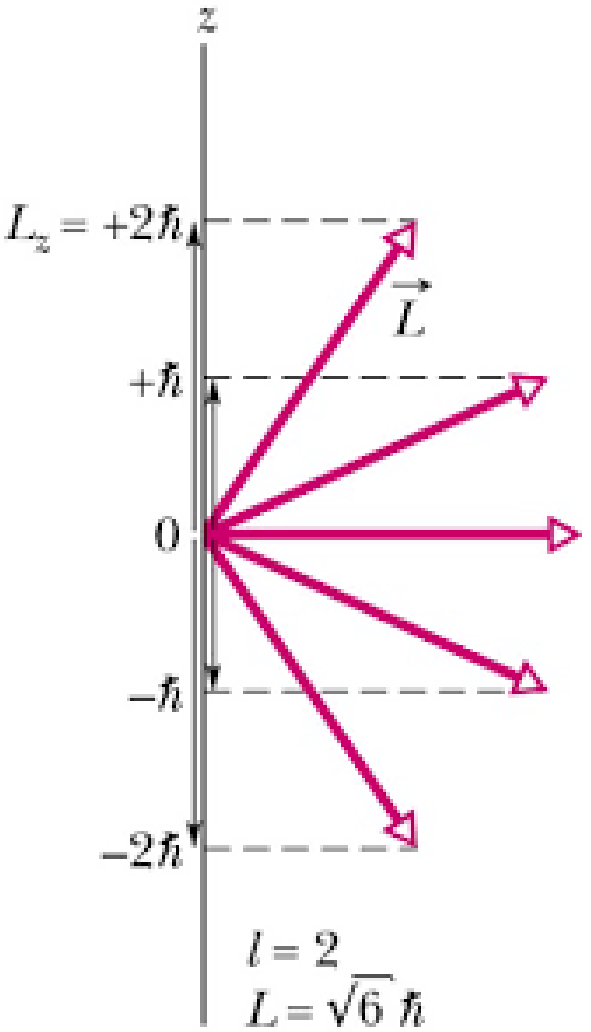
(Bild aus youtube:TheNilsor)

Was kann man messen?

Abgeschlossene quantenmechanische Systeme (Molekül, Atom, Kern, Elementarteilchen) haben erhaltenen Drehimpuls(-Betrag) $\sqrt{j(j+1)}\hbar$, wobei j eine Quantenzahl ist.
Man kann eine Komponente messen; traditionell ist das die Komponente in z-Richtung. Die $2j+1$ möglichen Messwerte sind

$$J_z = j\hbar, (j-1)\hbar, (j-2)\hbar, ..., (-j+1)\hbar, -j\hbar,$$

symmetrisch um den Wert Null im Abstand $\hbar$ verteilt.
Die beiden anderen Komponenten sind auf einige $\hbar$ genau messbar, was im Alltag natürlich nicht auffällt $\Rightarrow$ der Drehimpuls der Erde ist für praktische Zwecke in allen drei Komponenten hinreichend genau festgelegt.



(Uni Münster)

(Zur Notation: In der Quantenmechanik heißen „allgemeine“ Drehimpulse immer J, Bahndrehimpulse L und Spins S.)

Ungenauigkeit, etwas genauer (für Besserwisser)

Es gibt „quasiklassische“ quantenmechanische Zustände, für die die Messgenauigkeit besonders hoch ist, in der Regel diskutiert für den Spin.

Eine der Komponenten hat dann den maximal möglichen Wert $s\hbar$ (für ein System mit Spinquantenzahl s).

Die Richtung dieser Komponente muss nicht mit einer der Koordinatenachsen übereinstimmen.

Diese Komponente ist dann mit beliebiger Genauigkeit bekannt; die Unsicherheit dieses Messwerts ist dann Null:

$$\Delta S_{\parallel} = 0.$$

Die dazu senkrechten Komponenten sind nur mit einer gewissen Unsicherheit messbar:

$$\Delta S_{\perp} = \frac{\hbar}{\sqrt{2}}\sqrt{s} \ll \hbar s = S_{\parallel},$$

und für große Werte von s (1 Million...) ist diese Ungenauigkeit völlig vernachlässigbar.
(Solche Zustände nennt man kohärente Spinzustände, vgl. z.B. J.R. Klauder und B.-S. Skagerstam, Coherent States, World Scientific 1985)

Unendliche Weiten... der Hilbertraum...

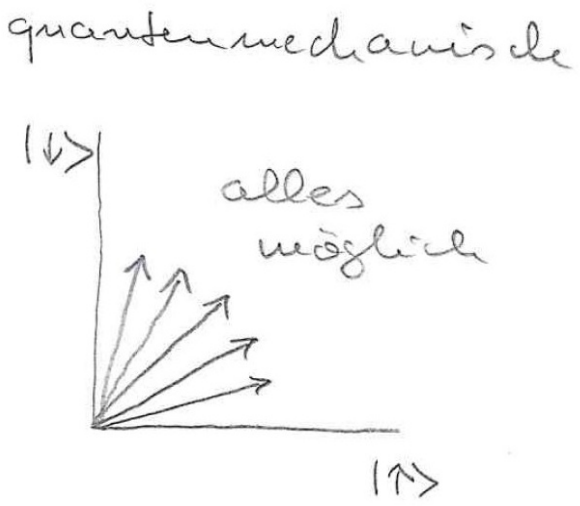
..ist für Spinsysteme eher endlich.

Den $2s+1$ möglichen Messwerten von S_z entsprechen $2s+1$ „grundlegend verschiedene“ Zustände des Spin-s-Systems.

Sie sind die Basiszustände in einem abstrakten $2s+1$-dimensionalen Raum über den komplexen Zahlen, dem Hilbertraum.

Der entscheidende Zug der Quantenmechanik ist es, dass das System jeden Zustand (Vektor) in diesem Raum einnehmen kann, nicht nur einen der Basis-Zustände, aber keinen Zustand außerhalb dieses Raumes.

Der kleinste interessante Hilbertraum hat offenbar zwei Dimensionen, entsprechend den beiden S_z-Messwerten $\pm\hbar/2$ für ein System mit Quantenzahl $s = 1/2$.
Dieser Hilbertraum ist tabu für Systeme mit einem Bahndrehimpuls und kann nur von Teilchen mit Eigendrehimpuls (Spin) besiedelt werden.



Was ist $|\uparrow\rangle, |\downarrow\rangle$? – Bitte noch etwas Geduld.

Wer hat Spin?

Sehr viele Elementarteilchen und aus ihnen zusammengesetzte Systeme, z.B. Atome und Atomkerne. Besonders einfach: Elektronen e, Protonen p und Neutronen n: alle haben die Quantenzahl

$$s = \frac{1}{2}.$$

Damit sind zwei Basis-Zustände möglich, die den Werten

$$S_z = \pm\frac{1}{2}\hbar$$

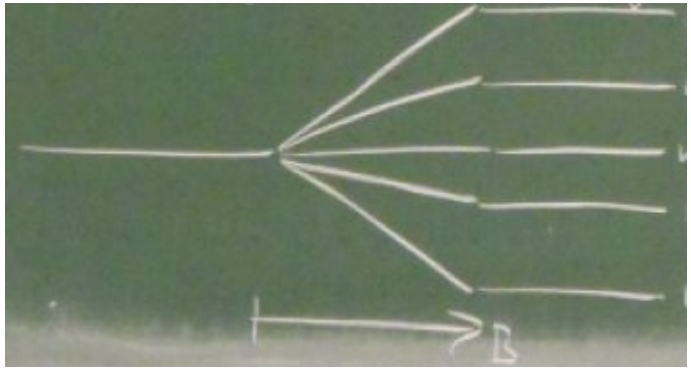
entsprechen. Der Hilbertraum ist also zweidimensional.

Die beiden Basis-Zustände entsprechen den zwei binären Zahlen 0 und 1, auf denen die gesamte Digitaltechnik beruht.

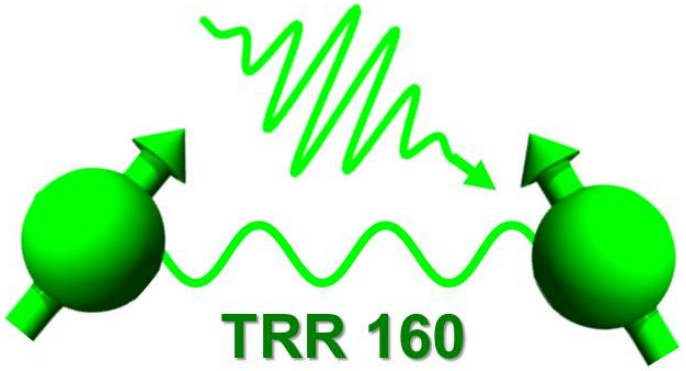
Idee: Quantensysteme mit Quantenzahl $s = \frac{1}{2}$ (Jargon: Spin-ein-halb-Systeme) als quantenmechanische Bits (Qubits) verwenden. Was die Folgen davon sind, werden wir gleich diskutieren.

Wie kann man Spins kontrollieren?

Elektronen, Protonen, Neutronen und viele Atomkerne besitzen ein zum Spin proportionales magnetisches Dipolmoment. In einem äußeren Magnetfeld $\vec{B}$ haben die verschiedenen Spin-Zustände dann unterschiedliche Energien (Zeeman-Effekt). Übergänge zwischen diesen Energieniveaus können durch Wechselfelder passender Frequenz herbeigeführt werden. ($\rightarrow$ Magnetische Kernresonanz NMR, Elektronenspinresonanz ESR)



Quanten von zirkular polarisiertem Licht tragen Drehimpuls $\hbar$ und können Übergänge zwischen Spin-Zuständen von (z.B.) Elektronen in Quantenpunkten herbeiführen.



Transregio-Sonderforschungsbereich

Dortmund-St. Petersburg

...und weitere komplexe spektroskopische Verfahren.

- Was ist Spin?
- Ist Spin anschaulich?
- Hilbertraum und Quanteninformation
- Anwendungen von Quanteninformation

Kann man den Spin „anschaulich“ verstehen?

Wenn das Elektron ein geladenes Kügelchen ist, wie schnell muss es sich dann drehen? Der „klassische Elektronenradius“

$$r_e = \frac{1}{4\pi\epsilon_0}\frac{e^2}{m_e c^2} = 2.8210^{-15} m$$

gibt an, „wie groß“ ein Elektron für eine einfallende elektromagnetische Welle „aussieht“.

Kann man den Spin „anschaulich“ verstehen?

Wenn das Elektron ein geladenes Kügelchen ist, wie schnell muss es sich dann drehen? Der „klassische Elektronenradius“

$$r_e = \frac{1}{4\pi\epsilon_0}\frac{e^2}{m_e c^2} = 2.8210^{-15} m$$

gibt an, „wie groß“ ein Elektron für eine einfallende elektromagnetische Welle „aussieht“.

Nimmt man diese Größe ernst, rotiert das Elektron am „Äquator“ mit mehr als 100facher Lichtgeschwindigkeit.
Darüber hinaus stellen Streuexperimente der Teilchenphysik, fest, dass das Elektron im Rahmen der Messgenauigkeit punktförmig ist, d.h. kleiner als 10^{-19}m, also eher kein Tennisball...

Kann man den Spin „anschaulich“ verstehen?

Wenn das Elektron ein geladenes Kügelchen ist, wie schnell muss es sich dann drehen? Der „klassische Elektronenradius“

$$r_e = \frac{1}{4\pi\epsilon_0}\frac{e^2}{m_e c^2} = 2.8210^{-15} m$$

gibt an, „wie groß“ ein Elektron für eine einfallende elektromagnetische Welle „aussieht“.

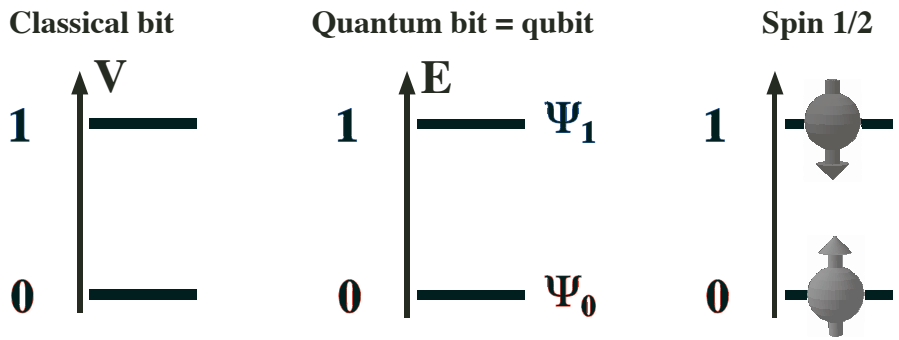
Nimmt man diese Größe ernst, rotiert das Elektron am „Äquator“ mit mehr als 100facher Lichtgeschwindigkeit.
Darüber hinaus stellen Streuexperimente der Teilchenphysik, fest, dass das Elektron im Rahmen der Messgenauigkeit punktförmig ist, d.h. kleiner als 10^{-19}m, also eher kein Tennisball...

Für ein viel größeres und schwereres Objekt, etwa einen Atomkern von ^{239}Pu ($s = \frac{1}{2}$) ergibt eine analoge Rechnung zwar nur eine Äquatorialgeschwindigkeit von 40 km/s; das Bild eines rotierenden Balls ist aber trotzdem falsch, denn der Spin des Pu-Kerns ergibt sich aus der Addition der 94 Protonenspins und 145 Neutronenspins nach den Regeln der Quantenmechanik. Das ist Kernphysik und führt hier zu weit.

- Was ist Spin?
- Ist Spin anschaulich?
- Hilbertraum und Quanteninformation
- Anwendungen von Quanteninformation

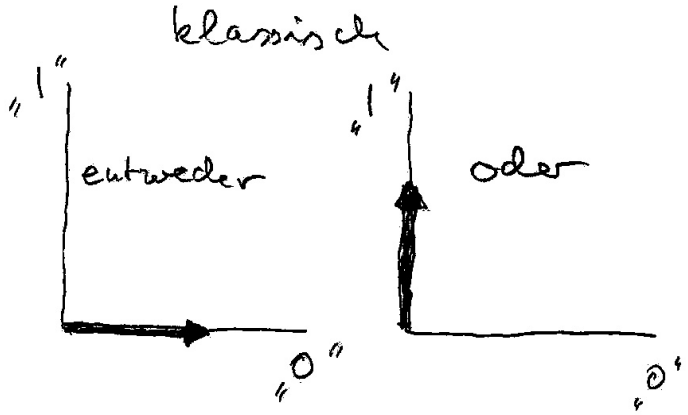
Unanschaulich, aber praktisch

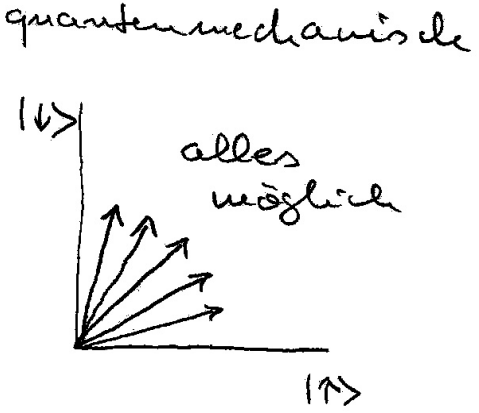
Zurück zum zweidimensionalen Hilbertraum eines Spin-1/2-Teilchens. Analogie zum klassischen Bit:



Entscheidend: Die beiden Zustände eines klassischen Bits schließen sich gegenseitig aus, das System kann also entweder in dem einen oder in dem anderen Zustand sein.

Dagegen sind die beiden Basiszustände eines Qubits eben genau das, nämlich die Basis eines Raums aus beliebigen Linearkombinationen der beiden Basiszustände.





Was folgt daraus?

A drop of the hard stuff: Etwas Formalismus

Die beiden Basiszustände eines Spin-1/2-Teilchens sind Zustände mit bestimmten Werten der Spinkomponente in z-Richtung: $S_z = \pm\frac{\hbar}{2}$. Diese Zustände sind Vektoren und wir schreiben sie „als Pfeile“ $|...\rangle$:

$$|+\hbar/2\rangle, |-\hbar/2\rangle \text{ oder kürzer } |\uparrow\rangle, |\downarrow\rangle.$$

Um die Analogie zu klassischen Bits zu betonen, benutzt man auch gern

$$|0\rangle, |1\rangle.$$

Ein beliebiger Vektor in dem durch diese Basiszustände aufgespannten Raum ist dann

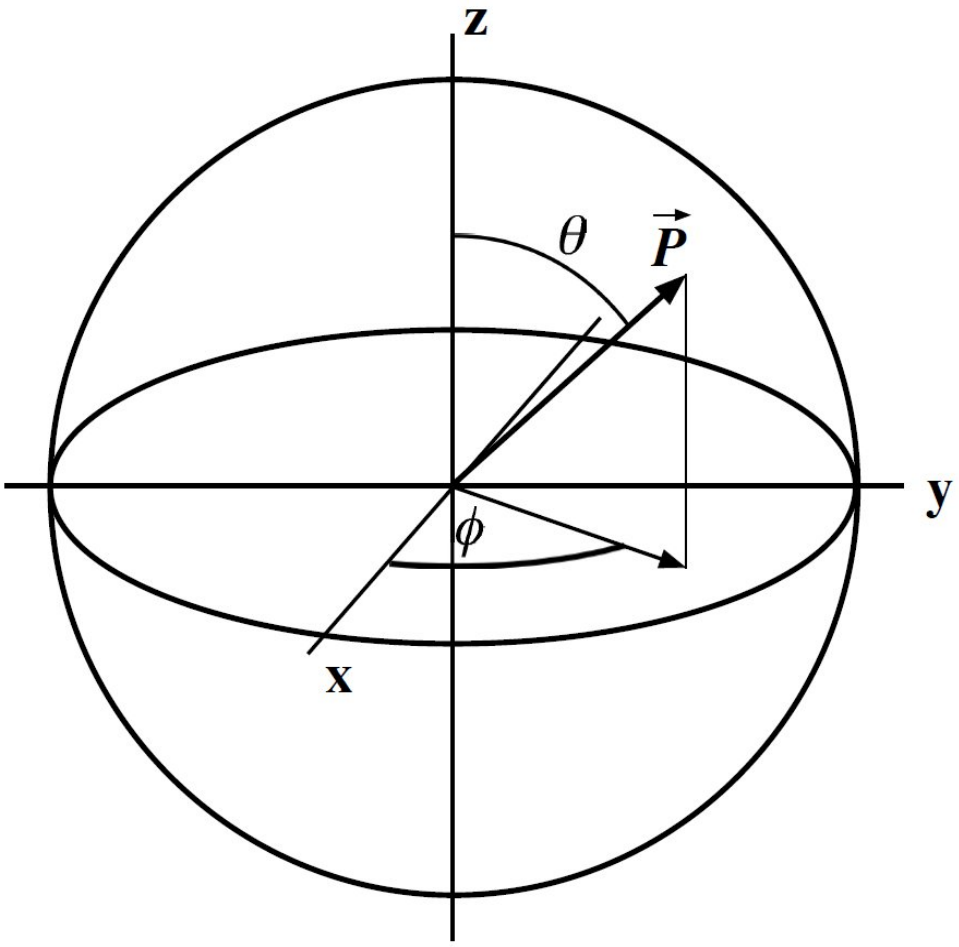
$$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle.$$

α und β sind komplex und durch die Normierungsbedingung $|\alpha|^2 + |\beta|^2 = 1$ miteinander verknüpft. Man kann dann den allgemeinen Zustand eines Spins 1/2 wie folgt schreiben:

$$|\theta, \varphi\rangle = \exp\left(-i\frac{\varphi}{2}\right)\cos\frac{\theta}{2}|\uparrow\rangle + \exp\left(i\frac{\varphi}{2}\right)\sin\frac{\theta}{2}|\downarrow\rangle \qquad (0 \leq \theta \leq \pi; 0 \leq \varphi \leq 2\pi).$$

Die beiden Winkel θ und φ kann man als geographische „Länge“ und „Breite“ auf einer Kugel interpretieren, der Bloch-Kugel.

$$|\theta,\varphi\rangle = \exp\left(-i\frac{\varphi}{2}\right)\cos\frac{\theta}{2}|\uparrow\rangle + \exp\left(i\frac{\varphi}{2}\right)\sin\frac{\theta}{2}|\downarrow\rangle \qquad (0 \le \theta \le \pi; 0 \le \varphi \le 2\pi).$$



Der „Nordpol“ $\theta = 0$ entspricht dem Basiszustand $|\uparrow\rangle$, der „Südpol“ $\theta = \pi$ entspricht dem Basiszustand $|\downarrow\rangle$; bei diesen beiden Zuständen ist der Phasenwinkel φ unwichtig.

Der Informationsgehalt eines Qubits

Ein klassisches Bit entspricht einer einzigen binären Ziffer, also der Antwort auf eine ja/nein-Frage.

Der allgemeine Zustand eines Qubits ist durch zwei Winkel (θ, φ) gegeben, „speichert“ also zwei reelle Zahlen. Das ist im Prinzip unendlich viel mehr Informationsgehalt als in einem klassischen Bit steckt. (Z.B. ist die relle Zahl $\pi = 3.14159265358979323846264338327950288419716939937510582097494459230781640628 62....)$

Wie man diese Information nutzt, kontrolliert verändert, speichert usw.: Inhalt der Quanteninformationsverarbeitung.

Trotz „unbegrenzter“ Speicherkapazität kein Grund zur Euphorie, denn

- Quanteninformation kann nicht kopiert werden. (No-Cloning-Theorem)
- Die zwei Winkel (θ, φ) sind nicht einfach zu messen (vorsichtig ausgedrückt), und schon gar nicht mit unendlicher Genauigkeit.
- Unvermeidbare Wechselwirkungen (Messungen müssen möglich sein) mit der Umgebung verändern die Quanteninformation.

Die Janus-Natur der Quanteninformation

Die Quanteninformation hat (mindestens) zwei Gesichter:

- Sie ist sehr empfindlich.
  (Dekohärenz, Wechselwirkungen mit Umgebung)

- Sie ist sehr sicher.
  (No Cloning $\longrightarrow$ Interesse von Bankern, Geheimdiensten)

- Sie ist sehr mächtig.
  (Quantencomputer zur Lösung extrem komplexer Probleme)

- Was ist Spin?
- Ist Spin anschaulich?
- Hilbertraum und Quanteninformation
- Anwendungen von Quanteninformation

Frühe Euphorie über Quantencomputer

COVER STORY

Beyond the PC: Atomic QC

Quantum computers could be a billion times faster than Pentium III

By Kevin Maney
USA TODAY

Around 2030 or so, the computer on your desk might be filled with liquid instead of transistors and chips. It would be

It wouldn't operate on anything so mundane as physical laws. It would employ quantum mechanics, which quickly gets into things such as teleportation and alternate universes and is, by all accounts, the weirdest stuff known to man.

Warum Quantencomputing ?

Quantencomputer können alles...

Warum Quantencomputing ?

Quantencomputer können alles...

...aber was können sie besser ?

Warum Quantencomputing ?

Quantencomputer können alles...

...aber was können sie besser ?

Für Quantencomputer geeignete Probleme:

viele mögliche Fälle müssen untersucht werden ($\rightarrow$ Quanten-Parallelismus), aber

nur wenige Ergebnisse sind gefragt.

Prominenteste Beispiele:

- Suche in einer unstrukturierten Datenbasis (Nadel im Heuhaufen)
  $\rightarrow$ Grover's Suchalgorithmus

- Globale Eigenschaft einer Funktion ("Ist $f(2l+1) > 0$ für alle l ?")
  $\rightarrow$ Shor's Faktorisierungsalgorithmus

Quantenparallelismus am Beispiel

Aufgabe: Berechne die Werte der vorgegebenen Funktion $f(n)$ für $0 \leq n \leq 1023$
in deutlich weniger als 1024 Operationen.

Verfügbar: Ein Quantenregister mit 10 Qubits zur Speicherung der Zahlen n und die quantenmechanische Implementation der Funktion f; dazu die Hadamard-Operation $\hat{H}$ (s.u.).

Schritte:

1) Initialisiere das Quantenregister in den Zustand

$$|\uparrow\rangle \otimes |\uparrow\rangle \otimes ... \otimes |\uparrow\rangle = |00...0\rangle.$$

2-11) Wende auf jedes der 10 Qubits die Hadamard-Operation $\hat{H}$ an.

$$\hat{H}|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle), \qquad \hat{H}|\downarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle)$$

(In Matrix-Schreibweise ist

$$\hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \Rightarrow \hat{H}|\uparrow\rangle = \hat{H}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$ usw.)

Ergebnis:

$$\frac{1}{(\sqrt{2})^{10}}\Big(|0\rangle+|1\rangle\Big)\otimes\Big(|0\rangle+|1\rangle\Big)\otimes\ldots\otimes\Big(|0\rangle+|1\rangle\Big)$$

$$=\frac{1}{32}\left(\underbrace{|0\ldots00\rangle}_{0}+|0\ldots01\rangle+|0\ldots10\rangle+\ldots+\underbrace{|1\ldots11\rangle}_{1023}\right)$$

also eine gleichgewichtige Kombination aller Zahlen von 0 bis 1023 in Binärform.

12) Wende nun einmal die Operation an, die die Berechnung von f für das 10-Qubit-Register implementiert.

Ergebnis:

$$\frac{1}{(\sqrt{2})^{10}}\Big(|0\rangle+|1\rangle\Big)\otimes\Big(|0\rangle+|1\rangle\Big)\otimes\ldots\otimes\Big(|0\rangle+|1\rangle\Big)$$

$$=\frac{1}{32}\left(\underbrace{|0\ldots00\rangle}_{0}+|0\ldots01\rangle+|0\ldots10\rangle+\ldots+\underbrace{|1\ldots11\rangle}_{1023}\right)$$

also eine gleichgewichtige Kombination aller Zahlen von 0 bis 1023 in Binärform.

12) Wende nun einmal die Operation an, die die Berechnung von f für das 10-Qubit-Register implementiert.

Fertig!

Spione...

- wollen Codes brechen ($\rightarrow$ Shor-Algorithmus, Primfaktorzerlegung).
- wollen abhörsichere Codes entwickeln (hier nicht behandelt).

Bei *beidem* hilft die Quantenmechanik!

Heute gängige Codes (Kreditkartendaten im Internet etc.): Codes mit *öffentlichem Schlüssel*, d.h. jeder kann verschlüsseln, nur Empfänger kann entschlüsseln. Diese Codes benutzen zahlentheoretisch konstruierte Funktionen

$$f_a(x_i) = y_i; \quad x_i \in \text{Klartext}, y_i \in \text{verschlüsselter Text}, a \text{ Schlüssel; natürliche Zahlen.}$$

Dabei hängt die *Umkehrfunktion*

$$\tilde{f}_{(p,q)}(y_i) = x_i, \quad pq = a$$

von den Primfaktoren p und q von a ab, die nicht einfach zu finden sind.
(Man bestimme z.B. die Primfaktoren von 29083 ohne elektronische Hilfsmittel.)

Bekanntestes Verfahren auf dieser Grundlage: *RSA* (Ron Rivest, Adi Shamir, Leonard Adleman). Diese Verfahren bieten keine absolute Sicherheit, aber alle bekannten klassischen Verfahren zur Faktorisierung einer Zahl mit N Ziffern benötigen exponentiellen Aufwand

$$\text{Schrittzahl} \sim \exp(cN^{1/3}(\log N)^{2/3}),$$

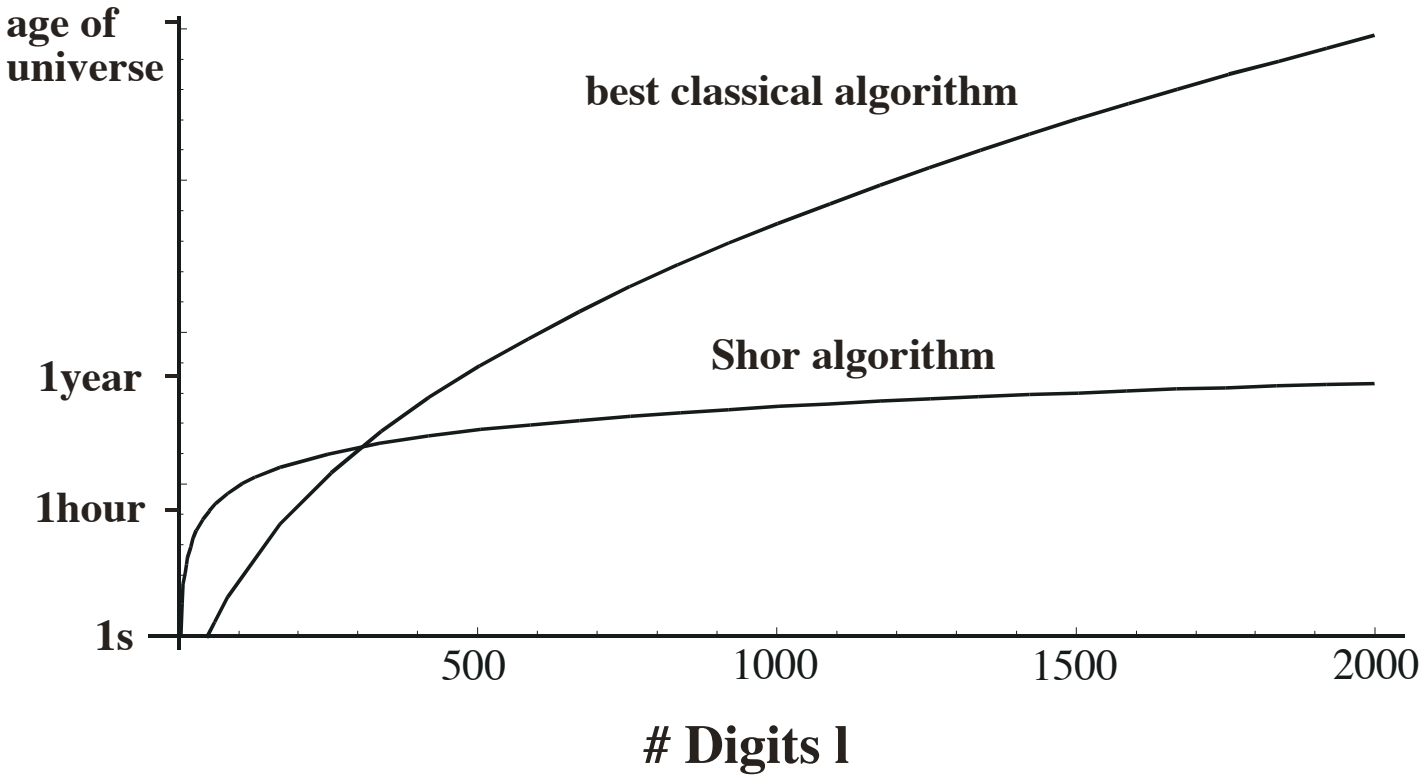
hingegen benötigt der Quanten-Algorithmus von Peter Shor nur polynomialen Aufwand:

$$\text{Schrittzahl} \sim N^2(\log N)(\log\log N)$$

1994 Peter Shor

P. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, in *35th Annual Symposium on Foundations of Computer Science*, IEEE Press, Piscataway, NJ (1994).

With his factoring algorithm, the computation time grows only algebraically, rather than exponentially with the number of digits.



Die zwei zentralen Elemente von Shor's Algorithmus:
Zahlentheorie → Faktorisierung durch Bestimmung der *Periode* einer gewissen Funktion
Quanten-Parallelismus → effiziente Periodenbestimmung durch *Quanten-Fouriertransformation* (QFT, noch schneller als FFT)
Annahme im Bild links: Bei 50 Ziffern braucht man klassisch 1 sec zum Faktorisieren, quantenmechanisch 1 h; ⇒ bei 300 Ziffern brauchen beide Verfahren 2.5 Tage,...

So geht's:

- Gesucht ist ein Primfaktor von N (groß; ungerade).

- Wähle eine zu N teilerfremde Zahl a.

  (Teilerfremdheit kann ohne Berechnung der Teiler festgestellt werden: GGT-Bestimmung nach Euklid.)

- Berechne die modulare Exponentialfunktion

$$F_N(x) = a^x \text{mod } N$$

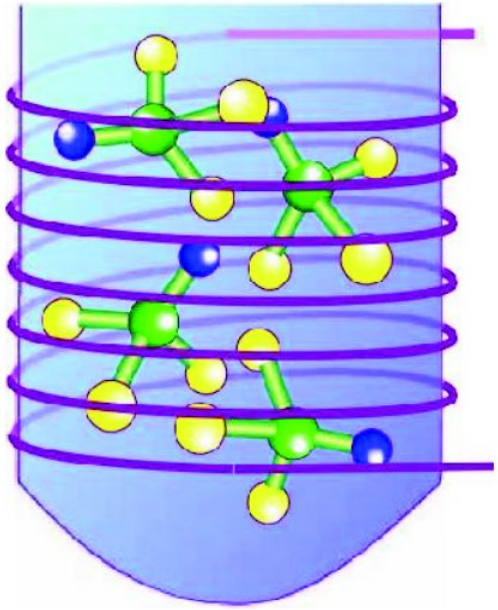
  für viele (z.B. N) natürliche x parallel.

- $F_N(x)$ ist periodisch mit Periode $r \leq N$.
  Bestimme mit Quantenfouriertransformation die Periode r.

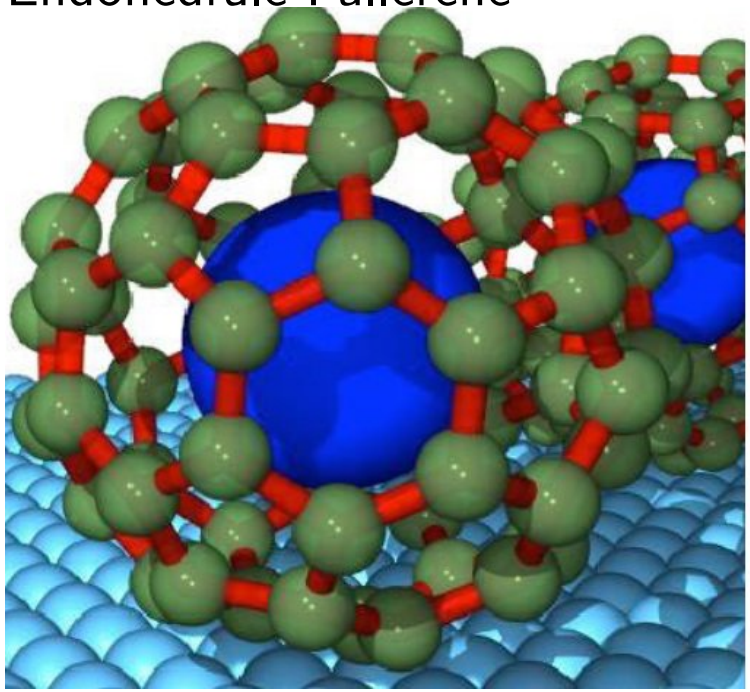
- Wenn r gerade und $a^{r/2} \text{mod } N \neq N - 1$ ist,
  dann ist einer der GGT von N und $a^{r/2} \pm 1$ ein Faktor von N.
  Die Eintretenswahrscheinlichkeit für diesen Fall ist 3/4, die Misserfolgswahrscheinlichkeit bei $m \to \infty$ Versuchen mit dem Algorithmus ist also $(1/4)^m \to 0$.

Quanten-Hardware

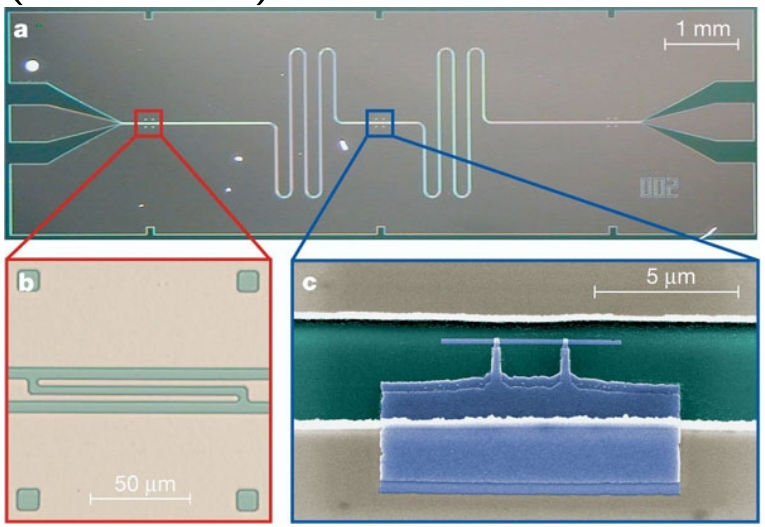
Kernspin-Resonanz



Endohedrale Fullerene

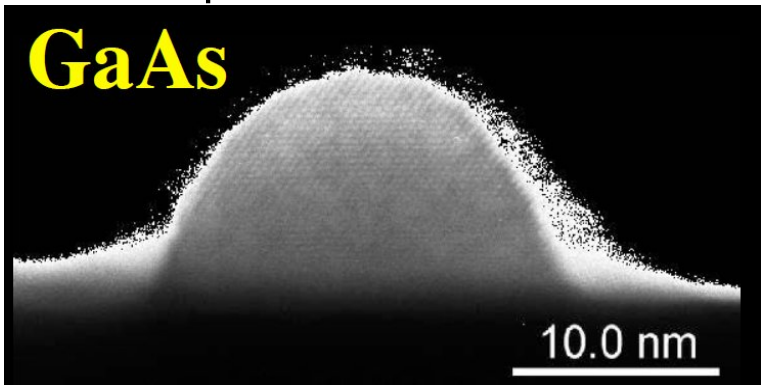


Supraleitende Mikrostruktur (Transmon)

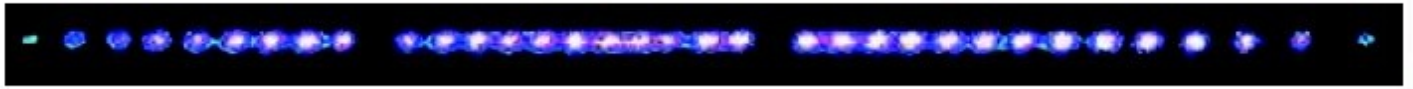


ETH Zürich

Quantenpunkt

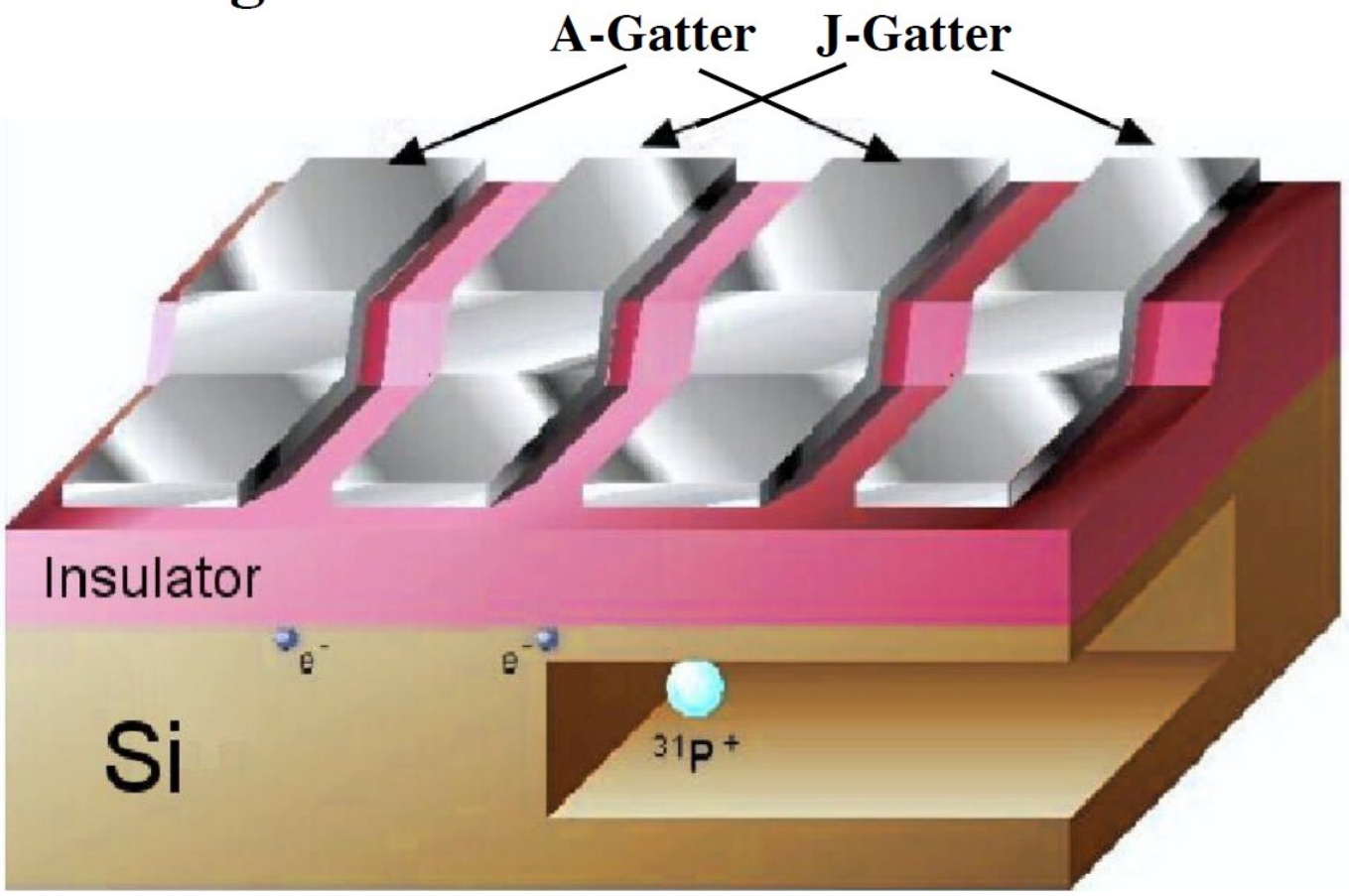


Gefangene Ionen



^{31}P in ^{28}Si

Vorschlag: *B.E. Kane, Nature 393, 133-137 (1998).*



Platz für Ihre Idee:

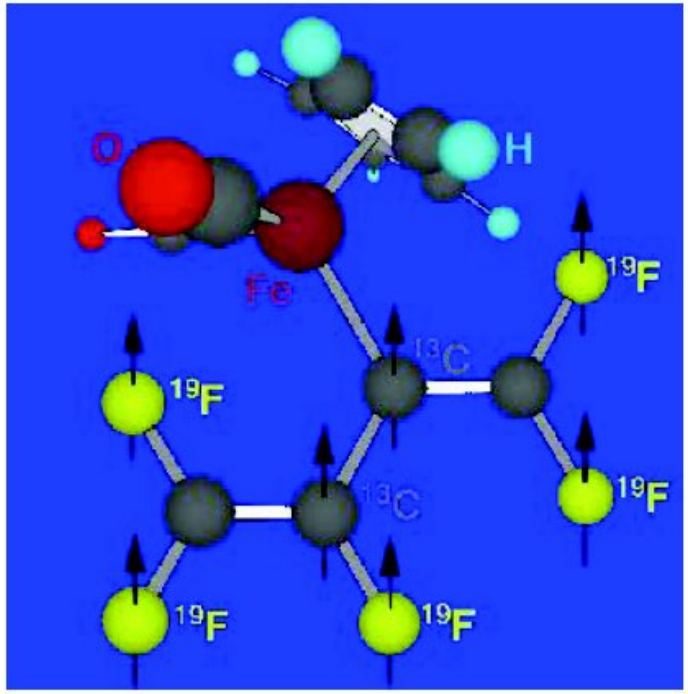
Eine Quanten-Rechnung

Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance

Lieven M. K. Vandersypen*†, Matthias Steffen*†, Gregory Breyta*, Costantino S. Yannoni*, Mark H. Sherwood* & Isaac L. Chuang*†

* *IBM Almaden Research Center, San Jose, California 95120, USA*
† *Solid State and Photonics Laboratory, Stanford University, Stanford, California 94305-4075, USA*

Nature 414, 883 (2001).



$$15 = 3 \times 5$$

Weitere Möglichkeiten

PRL **103,** 150502 (2009) PHYSICAL REVIEW LETTERS week ending 9 OCTOBER 2009

Quantum Algorithm for Linear Systems of Equations

Aram W. Harrow,[1] Avinatan Hassidim,[2] and Seth Lloyd[3]

[1]*Department of Mathematics, University of Bristol, Bristol, BS8 1TW, United Kingdom*
[2]*Research Laboratory for Electronics, MIT, Cambridge, Massachusetts 02139, USA*
[3]*Research Laboratory for Electronics and Department of Mechanical Engineering, MIT, Cambridge, Massachusetts 02139, USA*

(Received 5 July 2009; published 7 October 2009)

NSF WORKSHOP REPORT

QUANTUM INFORMATION AND COMPUTATION FOR CHEMISTRY

2016

(NSF=United States National Science Foundation)

Credit Risk Analysis using Quantum Computers

Daniel J. Egger,[1] Ricardo García Gutiérrez,[2] Jordi Cahué Mestre,[2] and Stefan Woerner[1,*]

[1] *IBM Research – Zurich*

[2] *IBM Spain*

(Dated: July 9, 2019)

We present and analyze a quantum algorithm to estimate credit risk more efficiently than Monte Carlo simulations can do on classical computers. More precisely, we estimate the economic capital requirement, i.e. the difference between the Value at Risk and the expected value of a given loss distribution. The economic capital requirement is an important risk metric because it summarizes the amount of capital required to remain solvent at a given confidence level. We implement this problem for a realistic loss distribution and analyze its scaling to a realistic problem size. In particular, we provide estimates of the total number of required qubits, the expected circuit depth, and how this translates into an expected runtime under reasonable assumptions on future fault-tolerant quantum hardware.

Platz für Ihre Idee:

Credit Risk Analysis using Quantum Computers

Daniel J. Egger,[1] Ricardo García Gutiérrez,[2] Jordi Cahué Mestre,[2] and Stefan Woerner[1,*]

[1] *IBM Research – Zurich*
[2] *IBM Spain*

(Dated: July 9, 2019)

We present and analyze a quantum algorithm to estimate credit risk more efficiently than Monte Carlo simulations can do on classical computers. More precisely, we estimate the economic capital requirement, i.e. the difference between the Value at Risk and the expected value of a given loss distribution. The economic capital requirement is an important risk metric because it summarizes the amount of capital required to remain solvent at a given confidence level. We implement this problem for a realistic loss distribution and analyze its scaling to a realistic problem size. In particular, we provide estimates of the total number of required qubits, the expected circuit depth, and how this translates into an expected runtime under reasonable assumptions on future fault-tolerant quantum hardware.

Platz für Ihre Idee:

Vielen Dank für Ihre Aufmerksamkeit!